Method for Creating and Reading a New Certificate Types for Certification of Keys

Related Patent Applications

U.S. Patent Application, Serial # 09/109,578 filed on July 2, 1998 and entitled "Inter Operability of Key Distribution Services", the contents of which application is hereby incorporated by reference.

U.S. Patent Application, Serial #09/274,525, filed on March 23, 1999 and entitled "Secure Hash-And-Sign Signatures", the contents of which application is hereby incorporated by reference.

Field of the Invention

The present invention relates to a method for creating a new certificate, the storage of that certificate on storage media (in particular on chipcards) and the reading of the certificate.

Background of the Invention

The idea underlying the use of the new certificate is the one-time, centralized authentication of a user or a service by an institution created for that purpose, termed a certification body. If the requirements of the certification body for successful identity verification are met, the certification body appends its own electronic signature to the public key of the identified person or service. The advantage for the subscribers to a public network lies in the fact that they only need to trust

the signature of the certification body, and in this way can be sure of the authenticity of the presented public key.

The certificate consists of two parts. The first part, for example, contains data elements relating to the key, the issuer of the certificate, the user, the signature algorithm, the serial number, etc. The second part of the certificate contains a digital signature generated using the first part of the certificate. A digital signature basically establishes the authenticity of electronically transmitted messages or electronic documents. In the process of generating a digital signature a HASH algorithm is used to form a HASH value from the first part of the certificate. The HASH algorithm compresses the data of the first part of the certificate. The HASH value is decrypted with a crypto algorithm. Decryption is based on the private key of a key pair.

A series of cryptographic keys are issued to a person or an institution for various purposes. These purposes include secure network communication, e.g.

- digital signature with legal recognition
- encryption of a document key
- verification of a user of an application based on a digital signature.

The possibilities for use of a key are defined in a single certificate which is digitally signed by the certification body.

At present, each digital key issued to a person or institution must be assigned a certificate. The certificates enable communication partners to verify the legitimate use of a key.

Each such certificate requires approximately 800 to 4000 bytes of data, including the certification body's digital signature. If, for example, three keys are to be stored on one chipcard in certified form, 2400 to 12000 bytes of space are required for the certificates. Fig. 1 shows the conventional storage of keys on a chipcard. For each key (1-3) a certificate is issued and stored on the chipcard. It is not possible to issue more than one key by means of one certificate and store it on the chipcard.

The issue of individual certificates for each key used means more memory is required on the keyholder's storage media. Furthermore, each certificate must be transmitted to the various communication partners of the keyholder and stored by them on their systems. The certificates also need to be stored on the various X.500 servers in the network and within the certification body in publicly accessible certificate lists. Which data fields may be redundant in several certificates is shown in Fig. 2.

The fact that one certificate is required per key results in an increased communication demand per transaction and increased memory requirement at all the communication partners. When the certificate expires, applications are made for new separate certificates for all keys, and the certificates are issued by the certification body.

It is therefore the object of the present invention to deliver a new form of the certificate which can be transmitted fast to the various communication partners and results in reduced memory requirement on the storage media.

Brief Description of the Invention

In accordance with the present invention, a new certificate type is provided. With the new certificate type, several certificates, containing a minimum quantity of redundant data fields, are collated to form one certificate and all redundant information on the certificates is eliminated. An embodiment of the new certificate type is the group certificate. The group certificate is particularly suitable where several keys are to be issued at the same time for the same user by the same certification instance. By means of the group certificate, all redundant data elements are eliminated and all data elements for a set of several keys subject to certification are grouped into one certificate. This substantially reduces the memory requirement, and handling of the certificates is simplified for the communication partners. A further embodiment of the new certificate type is the basic and supplementary certificate combination. This form of certification is suitable where certificates are issued at different times for the same user by the same certification body. The memory requirement is consequently somewhat more than for group certificates, but greater flexibility is gained in use of the keys.

Brief Description of the Drawings

The present invention is described in more detail on the basis of preferred embodiments in conjunction with drawings, wherein

Fig. 1 shows the conventional certification of keys according to the state of the art.

Fig. 2 shows the fundamental principle of the invention based on the certification as shown in Fig. 1.

Fig. 3 shows the group certificates for the keys in accordance with the invention according to Fig. 1.

Fig. 4 shows the structure of the basic and supplementary certificates in accordance with the invention.

Fig. 5 shows the method of creating the group, basic and supplementary certificates in accordance with the invention.

Fig. 6 shows the method of reading the group, basic and supplementary certificates in accordance with the invention.

Fig. 7 is a block diagram of a computer system which the present invention is applicable.

Fig. 8 is a block diagram of a network to which the present invention is applicable.

Detailed Description of the Invention

Fig. 1 presents the conventional certification of keys. A certificate is issued for each key. The certificate consists of two parts. The first part contains information (data elements) relating to the certification body (issuer of the certificate), the user of the certificate and the certified keys. These data elements include information relating to the key, the issuer of the certificate, the user, the signature algorithm, the serial number, etc. The second part contains a digital signature relating to the first part of the certificate. Table 1 describes

the possible components of the first part of a certificate based on an example.

Table 1

Component	Byte	Description
1	0	Bit 7 : 0= private key 1= Public key Bit 6-0: Key identification
2	1	Algorithm identification
3	2	Hash algorithm identification
4	3	Padding algorithm identification
5	4	Use of byte 0
6	5	Use of byte 1
7	7	Nominal key length in bits
8	9	Length of a data block
9	10	Length of a signature
10	11	Length of user information
11	12	User information
12	13	Length of key data
13	15	Key data

Component 1 of the certificate indicates whether the cryptographic key being certified is a public or private key. Component 1 of the first part of the certificate also contains a key identification. It specifies permitted applications of the cryptographic key contained in the certificate. If, after successful certification, the cryptographic key is to be used to execute a specific application, a request is made for this key identification and a check is made as to whether the certified key is usable for the specific application. Depending on the result of this request, the cryptographic key can then either be

used or an error message is generated.

With the aid of the following components 2, 3 and 4, algorithm identifications are specified. Component 2 indicates the asymmetric cryptographic methods for which the key being certified is suitable. In use of the certified key, a hash algorithm and/or a padding algorithm can be used, for example. This is defined with the aid of components 3 and 4.

With the aid of components 5 and 6 application areas of the cryptographic key can be defined. For example, component 5 can be used to determine that the cryptographic key may be used only to generate electronic signatures. Component 7 gives an indication in bits of the length of the cryptographic key to be certified with the certificate. With the aid of components 8, 9 and 10 block length data are transmitted as information for a user of the cryptographic key.

Component 11 delivers text information on the cryptographic key. This may, in particular, be instructions for use or security instructions for the user. Component 12 indicates the actual length of the cryptographic key to be certified. The key data are located in component 13.

When the first part of the certificate has been generated based on table 1, the process continues with creation of the second part of the certificate as presented in Fig. 1. To this end, an electronic signature of the first part of the certificate is generated. An electronic signature basically establishes the authenticity of electronically transmitted messages or electronic documents.

Fig. 2 shows the basic principle of the present invention. Several certificates, containing a minimum quantity of redundant information (data fields), are collated to form one certificate. The data fields framed in Fig. 2 mark the redundant data fields in the certificates being issued. In the present example the data fields: name of issuer, X.509 version, signature algorithm, issuer ID, user ID, user name and validity of the key are identical. The only differences are the respective certificate keys.

In this case the certificate keys 1-3 with the above-cited identical data fields are collated in one certificate where several keys are to be certified at the same time for the same user by the same certification body. Fig. 3 shows the result of this collation of identical and differing data fields (group certificate). This so-called group certificate is usually only issued where several keys are issued at the same time by the same certification body for the same user with identical validity periods. This is illustrated by the following example.

A legal entity applies for simultaneous issue of a certificate for several keys. After verification of the person a certificate (group certificate) is issued for all private keys for which application has been made. This certificate includes all keys and is signed by the certification body. All keys have a uniform period of validity. In comparison with a X.509 V 3 certificate (state of the art), only the additional information concerning the number of keys needs to be incorporated. This group certificate thus has the following data fields:

Name of issuer
Issuer ID
Name of user
User ID
Type/version of certificate
Number and types of keys
Public key
Serial number of the public key
Validity
Extensions
Digital signature of the certification body

If the same user applies for keys at different times from the same certification body, the method in accordance with the invention is executed such that the certification body issues to the user a basic certificate for all keys and a supplementary certificate for each key. The basic certificate contains all redundant data fields and the supplementary certificate all differing data fields. This is illustrated by the following example in conjunction with Fig. 4.

A user applies for a single certificate. The certification body issues a basic and a supplementary certificate to the user. The basic certificate contains the following data fields:

Name of issuer (certification body)
Issuer ID
Name of user
User ID
Type/version of the certificates
Serial number of the basic certificate

Digital signature of the basic certificate from the certification body
The supplementary certificate contains the following data fields:
Signature algorithm
Public key
Serial number of the public key
Validity
Extensions
Serial number of the associated basic certificate
Digital signature of the supplementary certificate from the certification body

If the same user applies for an additional key, only an additional supplementary certificate is created for the key.

Fig. 5 shows the method of creating a certificate in accordance with the invention in the form of a flowchart.

1. The following information is provided for the preferentially menu-guided method:

- How many keys are to be certified

- Information on the user, e.g. user name, user ID

- Information on the certifying body, e.g. name of certification body, user ID of certification body

2. Based on the information obtained in step 1), the method checks whether more than one key is to be certified at one time.

3. If the check in step 2) reveals that more than one key is to be certified at one time, the appropriate number of key pair are created.

4. When the key pairs have been created in step 3), a joint certificate (group certificate) is created to certify the keys. The certificate preferentially contains the following data fields:

- Name of certification body
- User ID of certification body
- Name of user
- User ID of user
- Type/version of the certificate
- Number and types of keys
- Key
- Validity
- Serial number
- Extensions

5. Then a digital signature for the certificate is created. The details of this method are presented in the section relating to Fig. 1.

6. The digital signature is appended to the certificate.

7. The certificate with the digital signature is transmitted to the desired storage medium, which may be a chipcard. On the chipcard the certificate with the digital signature is stored in the chipcard's non-volatile memory (EPROM).

8. However, if the check in step 2) reveals that at present only one key is to be certified, the method checks whether a basic certificate is already available.

9. If a basic certificate is already available, it is loaded and the serial number of the basic certificate - if available - is read to the system RAM.

10. A key pair (public/private key) is created.

11. A supplementary certificate preferentially containing the following data fields is created:

- Signature algorithm
- Key
- Serial number of key
- Validity period of the certificate
- Extensions
- Serial number of the basic certificate

12. Then the method of digital signature is executed for the supplementary certificate as described in step 5) and the digital signature is appended to the supplementary certificate.

13. If step 9 reveals that no basic certificate is available, the in method accordance with the invention first creates a basic certificate with the following data fields:

- Name of certification body
- User ID of certification body
- Name of user
- User ID of user
- Serial number of the basic certificate

14. Then a digital signature for the basic certificate is created and appended to the basic certificate.

15. Then a key pair is created.

16. Then a supplementary certificate with the following data fields is created:

- Signature algorithm
- Key
- Serial number of key
- Validity period of the certificate
- Extensions
- Serial number of the basic certificate

17. A digital signature for the supplementary certificate is created and appended to the supplementary certificate.

Fig. 6 describes the method in accordance with the invention for reading the certificate created in Fig.5.

It is to be assumed in the following that a specific application sends a request to the chipcard asking it to sign a message. To sign the message the chipcard requires a key. As presented in Fig. 5, the relevant keys are stored in the relevant supplementary certificates on the chipcard. The method in accordance with the invention first checks whether there are basic certificates stored on the chipcard. If there are no basic certificates stored on the chipcard, this means that there are no input certificates. In such cases the requested signature key can only be stored in a group certificate. The method searches

through the group certificates stored on the chipcard to locate a suitable signature key and loads the identified group certificate into the chipcard's RAM. The signature key can now be taken from the certificate and used to sign the message. If the method ascertains that there are also basic certificates stored on the chipcard, it first searches through all stored supplementary certificates for the presence of a suitable signature key for the application in question and loads the supplementary certificate with the suitable signature key into the chipcard RAM. The method reads from the supplementary certificate the serial number of the basic certificate, searches for the corresponding basic certificate and reads it too into the chipcard RAM. The chipcard RAM now contains the basic certificate and the associated supplementary certificate with the suitable signature key.

The present invention is capable of running on any properly configured general purpose computer system, such as the one shown in Figure 7. Such a computer system 700 includes a processing unit (CPU) 702 connected by a bus 701 to a random access memory 704, a high density storage device 708, a keyboard 706, a display 710, and a mouse 712. Also attached to the CPU 702 by the bus 701, are a scanner 714 for scanning documents 716 into the computer 700; and CD-ROM and magnetic disc drivers 718 and 720 for entry of information from optical and floppy magnetic disc mediums 722 and 724 containing the program code and data of the present invention. An example of such a computer is an IBM Personal Computer of the International Business Machines Corporation, with a 500 Mhz Pentium processor of Intel Corporation operating under Microsoft Windows 98 operating system of the Microsoft Corporation.

The computer 700 also contains a modem 726 for telecommunication of information 728 on the Internet and other networks. As shown in Figure 8, computers 700, like the one described above, are connected together in a network 800 by a server 802 that can be used to exchange information and one computer can access information contained in another. The database search engine and the checking and updating software, may be permanently located on all computers of the network, or can be on one computer, say computer 7, and transmitted through the medium of electromagnetic signals from that one computer to the other computers on the network when it is to be accessed and modified.

The advantages of the present invention lie in the fact that by the creation of a group certificate, and of basic and supplementary certificates, the size of the certificates can be decisively reduced and handling of the certificates by the holders and their communication partners is simplified. The group certificates with three keys save 1200 to 10000 bytes of memory space for the certificates.

For the basic and supplementary certificates additional shorter supplementary certificates (key certificates) per key are issued in addition to the basic certificate. This means somewhat more space is taken up than by the group certificates, but greater flexibility is provided in use of the keys.

It should be clear to those skilled in the art that a number of changes can be made in what has been disclosed without departing from the invention. Therefore, it should be understood that the present invention is not limited to the disclosed embodiment but includes within its scope those embodiments encompassed by the spirit and scope of the appended claims.